CS²SAT
Control System Cyber Security Self-Assessment tool

Homeland Security

CONTROL SYSTEM CYBER SECURITY SELF-ASSESSMENT TOOL

Purpose

The Control System Cyber Security Self-Assessment Tool (CS²SAT) provides users with a systematic and repeatable approach for assessing the cyber security posture of their industrial control system networks. The CS²SAT was developed under the direction of the Department of Homeland Security (DHS) Control Systems Security Program (CSSP) by cyber security experts from national laboratories and with assistance from the National Institute of Standards and Technology. The CS²SAT is a desktop software tool which guides users through a step-by-step process to collect facility specific control system information and then makes appropriate recommendations for improving the system's cyber security posture. The tool pulls its recommendations from a database of the best available cyber security practices, which have been adapted specifically for application to industry control system networks and components. Each recommendation is linked to a set of actions that can be applied to remediate specific security vulnerabilities.

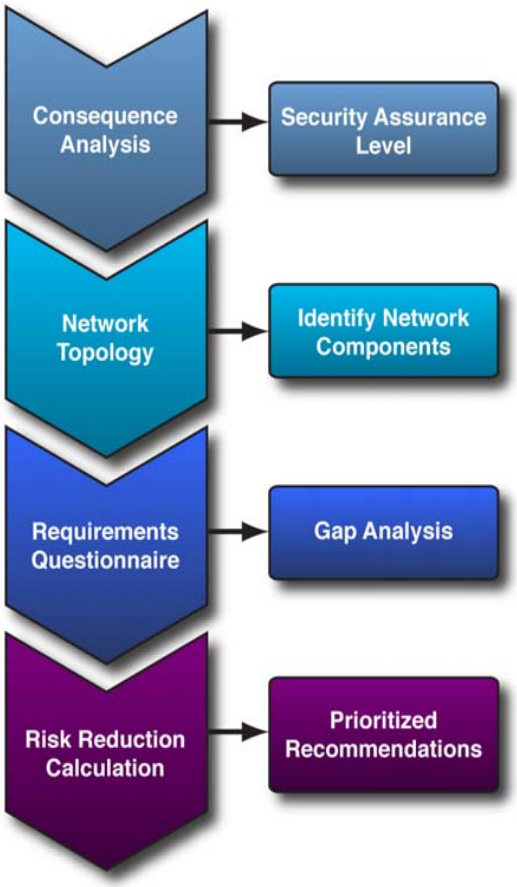
How it Works

The CS²SAT has four elements (see diagram):

- ***Consequence Analysis*** helps the user analyze the criticality of a site or facility relative to the potential consequences of a successful cyber attack. This element contains a questionnaire about potential losses related to economic impacts, deaths or injury, and environment impacts that might result from a successful cyber attack on a control system. Once the user has responded to a series of questions, the Consequence Analysis element calculates a recommended security assurance level (SAL) for the facility or subsystem. The SAL indicates the level of rigor that might be required to protect against the anticipated consequences of a compromised system. The tool uses the calculated security assurance level to determine how the user measures up against the recommendations.

- ***Network Topology*** helps the user identify the network architecture and components that are critical to the system's cyber security boundary. This element of the tool contains a graphical user interface to define the cyber security boundaries and connectivity of the control system network. The tool's software contains icons for the various system components and allows the user to drag and drop the network topology into the tool.

- ***Requirements Questionnaire*** generates a set of questions based on the specific network topology and consequence analysis responses entered by the user. The user then selects the best answer to each question based on the control system's configuration and implementation of security polices and practices. Upon completion of the questionnaire, the CS²SAT provides a security gap report that compares the user's responses to the recommended security strategies. A graphical representation of the analysis is also provided so the user can easily identify areas that need improvement.



- ***Risk Reduction Calculation*** provides a prioritized list of control systems security recommendations from the results of the questionnaire. The recommendations provide the user with a systematic approach to address control systems security improvements based on the greatest potential to reduce the risk of a successful cyber attack.

Tool Development Status

The CS^{2}SAT team has collected and assembled a comprehensive set of cyber security requirements and associated strategies for compliance. These requirements have been collected from the best available and emerging standards in the control system community. They have been loaded into the tool's software, which provides a user-friendly interface for users to systematically retrieve requirements specific to their system network. The tool is currently in the beta testing phase with asset owners and system vendors. Testing has allowed the development team to improve the tool in preparation for a release to the control systems community. Those who have participated in the testing are identifying many areas for improving the cyber security posture of their control systems.

Getting Involved

If you are interested in learning more about the NCSD Control Systems Security Program (CSSP) and its efforts related to control systems security, visit the CSSP web site: http://www.us-cert.gov/control_systems/. For more information about the Control Systems Cyber Security Self Assessment Tool and how to improve the cyber security posture of your control system network, contact us at cs2sat@hq.dhs.gov.

Homeland Security

Contact Information

Email: cs2sat@hq.dhs.gov